This listing of claims replaces all prior versions, and listings, of claims in this application.

Listing of Claims:

1. (Cancelled)

2. (New): A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:

inserting into a kernel of the operating system a substitute process creation function;

intercepting a request for execution of an application executable by a user using the substitute process creation function;

communicating information about the request from the substitute process creation function to a user-mode application running as a service;

comparing the information to a list of authorized executables for the user using the user-mode application;

if the information does not match an item on the list, communicating a first message to deny the request from the user-mode application to the substitute process creation function; and

if the information does match an item on the list, communicating a second message to permit the request from the user-mode application to the substitute process creation function.

3. (New): The method of claim 2, wherein the inserting into a kernel of the operating system a substitute process creation function comprises:

creating a device driver;

loading the device driver into the kernel; and

modifying a table consulted by a dispatcher using the device driver, wherein the modifying a table causes the dispatcher to call the substitute process creation function in place of a second process creation function.

4. (New): The method of claim 3, wherein the loading the device driver comprises one of dynamically loading into the kernel and loading into the kernel as part of a boot sequence.

5. (New): The method of claim 2, wherein the substitute process creation function is a wrapper around a process creation function provided by the operating system.

6. (New): The method of claim 5, wherein the process creation function provided by the operating system comprises ZwCreateProcess.

7. (New): The method of claim 2, wherein the information comprises one or more of a user name, an application executable name, and a cryptographic identifier of an application executable.

8. (New): The method of claim 7, wherein the cryptographic identifier of an application executable comprises a hash created using an MD5 cryptographic algorithm.

9. (New): The method of claim 2, wherein the list comprises one or more of an application executable name and a cryptographic identifier of an application executable.

10. (New): The method of claim 2, wherein the comparing the information to a list comprises comparing an application executable name of the information with an application executable name of at least one item from the list.

11. (New): The method of claim 2, wherein the comparing the information to a list comprises comparing a cryptographic identifier of the information with a cryptographic identifier of at least one item from the list.

12. (New): The method of claim 2, wherein the communicating information about the request comprises one or more of releasing a semaphore, calling an application program interface function, polling, using a socket, and using a pipe.

13. (New): The method of claim 2, wherein the communicating a first message to deny the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe.

14. (New): The method of claim 2, wherein the communicating a second message to permit the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe.

15. (New): A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:

inserting into a kernel of the operating system a substitute process creation function;

intercepting a request for execution of an application executable by a user using the substitute process creation function;

communicating information about the request from the substitute process creation function to a user-mode application running as a service;

prompting the user for authorization to proceed using the user-mode application;

if the authorization is not provided, communicating a first message to deny the request from the user-mode application to the substitute process creation function; and

if the authorization is provided, communicating a second message to permit the request from the user-mode application to the substitute process creation function.

16. (New): The method of claim 15, wherein the authorization comprises a password.

17. (New): The method of claim 16, wherein the inserting into a kernel of the operating system a substitute process creation function comprises:

creating a device driver;

loading the device driver into the kernel; and

modifying a table consulted by a dispatcher using the device driver, wherein the modifying a table causes the dispatcher to call the substitute process creation function in place of a second process creation function.

18. (New): The method of claim 17, wherein the loading the device driver comprises one of dynamically loading into the kernel and loading into the kernel as part of a boot sequence.

19. (New): The method of claim 15, wherein the substitute process creation function is a wrapper around a process creation function provided by the operating system.

20. (New): A system for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:

a substitute process creation function, wherein the substitute process creation function is inserted into a kernel of the operating system and intercepts a request for execution of an application executable by a user; and

a user-mode application running as a service, wherein the a user-mode application receives information about the request from the substitute process creation function, compares the information to a list of authorized executables for the user, communicates a first message to deny the request to the substitute process creation function, if the information does not match an

item on the list, and communicates a second message to permit the request to the substitute process creation function, if the information does match an item on the list.

21. (New): The system of claim 20, further comprising an administrative server, wherein the administrative server is in communication with the user-mode application, and wherein the user-mode application downloads the list from the administrative server.